



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Am

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/018,359	12/19/2001	Hideki Matsushima	2001-1853	7850

513 7590 05/25/2005

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER

ELMORE, JOHN E

ART UNIT PAPER NUMBER

2134

DATE MAILED: 05/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/018,359	Applicant(s) MATSUSHIMA ET AL.	
	Examiner John Elmore	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 December 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 19 December 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All. b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>12/19/2001</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-8 have been examined.

Priority

2. Acknowledgment is made of applicant's claim for priority under 35 U.S.C. 120 to prior parent Application No. 09/568,551 filed on May 11, 2000.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. **Claims 1, 2 and 6-8 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Hall et al. (US 5,920,861), hereafter Hall, incorporating by reference Ginter et al. (US 5,892,900), hereafter Ginter.

Regarding claim 1, Hall discloses an apparatus comprising:

a reception unit (Hall, part of value chain participant 602; Ginter, distributor 106) operable to receive an encrypted digital work (Hall, DDS 200 and content 102 in secure container 100; Ginter, content object 300 in secure container 302) encrypted using a content key and the content key from the distribution apparatus (Hall, DDS provider 600; Ginter, content creator 102 or other distributor 106) (see Ginter, col. 36, lines 10-

Art Unit: 2134

43; col. 56, lines 6-16; col. 59, lines 8-15 and 28-54; col. 135, line 5, through col. 136, line 36; col. 223, lines 5-11; see Hall, col. 17, lines 1-12), the encrypted digital work belonging to one of a plurality of categories and all encrypted digital works belonging to a same category being digital works made up of a same logical data structure (Hall, DSS 200; col. 5, lines 26-46; col. 11, lines 15-49; col. 13, line 41, through col. 14, line 3),

a distinguishing unit (Hall, part of value chain participant 602; Ginter, distributor 106) operable to distinguish a category to which a received encrypted work belongs (Hall, category defined by DSS 200, so all works corresponding to a DSS are distinguished by category; col. 11, lines 15-47), and

a writing unit (Hall, part of value chain participant 602) operable to write the received encrypted digital work and the generated encrypted content key to an area assigned to the distinguished category in the storage area of the recording medium (see Hall, Fig. 6 and 7; col. 12, lines 15-18; col. 14, lines 13-24; and see Ginter, col. 18, lines 6-21; col. 56, lines 12-19; col. 135, lines 59-65).

But Hall does not explicitly explain a key encryption unit operable to encrypt the received content key using a key unique to the distinguished category and generate the encrypted content key.

However, Hall teaches that content is stored in data blocks (Ginter, 812) within a secure container (Hall, 100; Ginter, 302) that are defined by the creator or packager of the container (Ginter, lines 59-65) and that each data block is encrypted with a unique key (Ginter, col. 135, line 67, through col. 136, line 4; col. 199, lines 34-65). One of

Art Unit: 2134

ordinary skill in the art would recognize that a data block represents a category when such a block is sized to allow all of the content associated with that category to be placed within it and that it is a simple means to check the DDS for each content object to determine what content applies to each category. Further, the Examiner takes official notice that one of ordinary skill in the art would recognize that once the content of a category is placed with a data block, the key which encrypts the data block is the key which encrypts the category.

Therefore, it would be obvious for one of ordinary skill in the art at the time of the invention to provide a key encryption unit operable to encrypt the received content key using a key unique to the distinguished category and generate the encrypted content key. One would be motivated to do so to provide a simple means to secure access to content by its category, as in the example where a user is granted access to a first category content, such as a set of low-definition images, but not a secondary category content, such as a set of high definition images.

Regarding claim 2, the apparatus of Hall as applied to claim 1 is relied upon in regard to the teaching that the encrypted digital work includes type information showing the category, the reception unit receives the encrypted digital work which includes the type information showing the category, the distinguishing unit extracts the type information from the encrypted digital work and distinguishes the category using the extracted type information, and the key encryption unit uses a key unique to and corresponding to the extracted type information.

Hall further teaches that the writing unit includes:

Art Unit: 2134

a table storage unit operable to store in correspondence, for each category, type information showing the category, and an area name (location information 266) showing an area in the storage area to which the category is assigned (Hall, Fig. 7; col. 14, lines 13-24; Ginter, col. 135, lines 59-65), and

an area name extraction unit operable to extract the area name stored in correspondence with the extracted type information from the table storage unit (Hall, Fig. 7; col. 14, lines 13-29);

But Hall does not explicitly explain an access unit operable to write the received encrypted digital work to an area in the recording medium shown by the extracted area name.

However, Hall teaches that the content packager (Hall, participant 602; Ginter, content creator 102 or distributor 106) writes a secure container (Hall, 100; Ginter, 302) to a recording medium, including a smart card or portable semiconductor memory device (Ginter, col. 18, lines 6-21; col. 40, line 62-63; col. 134, lines 34-38). One of ordinary skill in the art would recognize that the extracted area name that defines the location of encrypted digital work within the secure container also defines the location of encrypted digital work on the recorded medium because the secure container itself is written to the recorded medium. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide an access unit operable to write the received encrypted digital work to an area in the recording medium shown by the extracted area name. One would be motivated to do so in order to simplify access to

Art Unit: 2134

the encrypted work by defining its location relative to the secure container that embodies it regardless of the medium on which the container is stored.

Regarding claim 6, this is a method version of the claimed apparatus above (claim 1), wherein all limitations have been addressed. Therefore, for reasons provided above, such claims also would have been obvious.

Regarding claim 7, this is a computer-readable-medium version of the claimed apparatus above (claim 1), wherein all limitations have been addressed. Therefore, for reasons provided above, such claims also would have been obvious.

Regarding claim 8, this is a program version of the claimed apparatus above (claim 1), wherein all limitations have been addressed. Therefore, for reasons provided above, such claims also would have been obvious.

4. **Claims 3-5 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Hall in view of Diffie et al. ("Authentication and Authenticated Key Exchanges," Designs, Codes and Cryptography, Kluwer Academic Publishers, 1992), hereafter Diffie.

Regarding claim 3, Hall teaches all the limitations of claim 2, and further teaches that the recording medium (Ginter, portable electronic appliance 600) further includes an apparatus authentication unit operable to authenticate a validity of the content reception apparatus, the storage area including a authentication area (Ginter, col. 254, lines 6-62; col. 255, lines 60-66), and

the content reception terminal apparatus further includes a medium authentication unit operable to authenticate a validity of the recording medium (Ginter, col. 8, lines 1-7; col. 12, lines 31-37; col. 212, lines 10-16).

But Hall does not explicitly explain that the writing means writes the encrypted content key to the area assigned to the distinguished category in the authentication area, when mutual authentication by the apparatus authentication unit and the recording medium authentication unit succeeds.

However, Hall teaches that the recording medium communicates securely with a party with which it exchanges information (Ginter, col. 259, lines 42-62) and that means of authentication are employed between parties exchanging secure containers (Ginter, col. 8, lines 1-7; col. 12, lines 31-37; col. 212, lines 10-16). And Diffie teaches a method of two-party mutual authentication using the exchange of digital signatures (page 9, first paragraph) prior to the transfer of content information for the purpose of enhancing security by assuring that each of the parties is authentic and not an imposter (page 2, paragraph 3).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Hall with the teaching of Diffie such that the writing means writes the encrypted content key to the area assigned to the distinguished category in the authentication area, when mutual authentication by the apparatus authentication unit and the recording medium authentication unit succeeds. One would be motivated to do so to enhance security by assuring that each of the parties is authentic and not an imposter.

Regarding claim 4, Hall teaches all the limitations of claim 3, but does not explain that the recording medium further stores type information specifying a type of the recording medium, the content reception terminal apparatus further includes: a type information storage unit operable to store type information showing a type of a recording medium permitting writing by the content reception terminal, a retrieval unit operable to retrieve type information from the recording medium, and a match judgment unit operable to judge whether the recorded type information and the retrieved type information match; and the writing unit prevents the writing when the match judgment unit judges the recorded type information and the retrieved type information not to match.

However, Hall teaches that the recording medium embodies on a variety of types (Ginter, col. 60, line 58, through col. 61, line 2; col. 255, lines 60-66) and further stores information used to verify its identity to the entity distributing information to it (col. 254, lines 50-52). One of ordinary skill in the art would recognize that information retrieved from the recording medium would include type information where different medium types are employable and must therefore be distinguished. One of ordinary skill in the art would further recognize that in the case where not all employable recording mediums are supported or otherwise permissible, the reception terminal apparatus would necessarily comprise a storage area containing a list of permissible recording mediums, a retrieval unit, and a matching unit operable to read the type information from the recording medium and compare it to the list of permissible types for the purpose of determining whether the writing operation may proceed normally.

Therefore, the Examiner takes official notice that it would be obvious to one of ordinary skill in the art at the time the invention was made to provide that the recording medium further stores type information specifying a type of the recording medium, the content reception terminal apparatus further includes: a type information storage unit operable to store type information showing a type of a recording medium permitting writing by the content reception terminal, a retrieval unit operable to retrieve type information from the recording medium, and a match judgment unit operable to judge whether the recorded type information and the retrieved type information match; and the writing unit prevents the writing when the match judgment unit judges the recorded type information and the retrieved type information not to match. One would be motivated to do so to determine whether the writing operation may proceed normally.

Regarding claim 5, Hall teaches all the limitations of claim 4, and further teaches that the distribution apparatus broadcasts the encrypted work and the content key on a digital broadcast wave, the content reception apparatus is a digital broadcast reception apparatus for receiving the digital broadcast wave, and the reception unit receives the digital broadcast wave, and extracts the encrypted digital work and the content key from the received digital broadcast wave (Ginter, digital broadcast; col. 3, lines 18-30; col. 56, lines 12-16).


Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JE


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100